Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada
Canada

National Security Guidelines for Research Partnerships

This publication is available online at https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre

Innovation, Science and Economic Development Canada

C.D. Howe Building

235 Queen Street

Ottawa, ON K1A 0H5

Canada

Telephone (toll-free in Canada): 1-800-328-6189

Telephone (international): 613-954-5031

TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Reproduction Authorization

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from the Department of Industry, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that the Department of Industry is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced or as having been made in affiliation with, or with the endorsement of, the Department of Industry.

For permission to reproduce the information in this publication for commercial purposes, please fill out the Application for Crown Copyright Clearance at www.ic.gc.ca/copyright-request or contact the ISED Citizen Services Centre mentioned above.

© His Majesty the King in Right of Canada, as represented by the Minister of Innovation, Science and Economic Canada 2019.

Cat. No. Iu37-36/2023E-PDF

ISBN 978-0-660-46919-5

Aussi offert en français sous le titre Lignes directrices sur la sécurité nationale pour les partenariats de recherche.

Table of Contents

Summary of National Security Guidelines for Research Partnerships

Domestic and international partnerships are an essential component of Canada's open and collaborative academic research, guided by the principles of academic freedom and institutional autonomy. The majority of research partnerships have transparent intentions that provide mutual benefits to all research partners. However, some activities by foreign governments, militaries and other actors pose real risks to Canada's national security and the integrity of its research ecosystem.

To address these risks, researchers, research institutions, federal granting agencies, and the Government of Canada have a shared responsibility to identify and mitigate any potential national security risks related to research partnerships.

To ensure the Canadian research ecosystem is as open as possible and as secure as necessary, the Government of Canada is introducing the ***National Security Guidelines for Research Partnerships.*** The purpose of the guidelines is to integrate national security considerations into the development, evaluation, and funding of research partnerships.

Developed in consultation with the Government of Canada-Universities Working Group, these guidelines are intended to help safeguard Canada's research ecosystem from foreign interference, espionage, and unwanted knowledge transfer that could contribute to: advancements in military, security, and intelligence capabilities of states or groups that pose a threat to Canada; or disruption of the Canadian economy, society, and critical infrastructure. The guidelines will:

Provide clear information on the specific national security considerations for research partnerships – including who researchers partner with and what areas of research are at higher risk – to support researchers, research institutions, and government funders to undertake consistent, risk-targeted due diligence to identify and mitigate potential national security risks to research; and,

Be supported by transparent information, communication, and resources from the Government of Canada as to the evolving scope and nature of these risks and how the research community can work to identify and mitigate these risks. Researchers are encouraged to identify and apply measures to minimize any potential or identified national security risks to safeguard their research and its outcomes.

All researchers are encouraged to use the National Security Guidelines for Research Partnerships to assess all research partnerships, with any partner or funder, to protect their work. The *National Security Guidelines for Research Partnerships* will be applied to federal research partnership funding starting with all applications to the Natural Science and Engineering Research Council's (NSERC) Alliance Grants involving a private sector organization partner.

It is important that all stakeholders in Canada's research ecosystem work collaboratively and in a manner consistent with Canadian laws, to identify, mitigate, and – in cases where the risks to Canadian interests cannot be sufficiently mitigated or outweigh the potential benefits – decline research partnerships that may assist those seeking to undermine Canada's national security. In doing so, Canada's research ecosystem will remain secure while pursuing open and collaborative research partnerships that benefit Canada, while safeguarding its national security interests.

National Security Guidelines for Research Partnerships

Canada's commitment to open and collaborative academic research embraces discovery, creativity and innovation while keeping Canadian research and training internationally competitive. Domestic and international partnerships are an essential component of this ecosystem, guided by the principles of academic freedom and institutional autonomy.

The majority of research partnerships are transparent and provide mutual benefits to all research partners. However, some activities by foreign governments, militaries and other actors pose real risks to Canada's national security and the integrity of its research ecosystem.

To address these risks, researchers, research institutions, federal granting agencies, and the Government of Canada have a shared responsibility to take measures to identify and mitigate any potential national security considerations.

That is why the Government of Canada is introducing *the National Security Guidelines for Research Partnerships*, developed in consultation with the Government of Canada-Universities Working Group, to integrate national security considerations into the development, evaluation, and funding of research partnerships.

Guiding Principles

The Government of Canada recognizes that Canada's research ecosystem needs to be as open as possible and as safeguarded as necessary so it benefits Canada, Canadians, and the global good. The federal government and stakeholders in the research enterprise have a shared responsibility to protect the integrity of the research ecosystem and safeguard it from activities that undermine the foundational principles of openness, transparency, merit, and reciprocity that underlie the research ecosystem in Canada.

The following principles are shared by the Government of Canada and the research community and guide these collaborative efforts to safeguard Canada's world-leading research ecosystem:

- **Academic Freedom**: Freedom to teach and conduct research in an academic environment. It is fundamental to the mandate of institutions to pursue truth, provide education to students, and disseminate knowledge and understanding. Academic freedom, like institutional autonomy, requires an environment of enabled autonomy in which researchers are free from undue external influence or limitations on scholarly inquiry.

- **Institutional Autonomy**: Research institutions are free to pursue inquiry and disseminate knowledge based on evidence, truth, and peer review. Institutions must be free to pursue their own mission based on the oversight of their governance to meet community as well as local needs. Institutional autonomy - along with academic freedom and freedom of expression - require a safe and secure environment in which all individuals and institutions are free from unwanted external influence.

- **Freedom of Expression**: As provided for in the *Canadian Charter of Rights and Freedoms*, freedom of expression is the protection of free speech and the open exchange of ideas that form the cornerstone of intellectual discourse and the engine of impactful discovery.

- **Equity, Diversity, and Inclusion**: Freedom from discrimination is a fundamental and internationally recognized human right that is necessary for all aspects of the research enterprise. It is the diversity of identity and thought, with room for a variety of ideas, cultures, and views. Ensuring that everyone, regardless of background or identity, is able to freely participate in the research ecosystem will help build an innovative, prosperous, and inclusive world.

- **Research in the Public Interest**: Research across all disciplines produces knowledge that can improve the quality of life and contribute to the public interest of Canadian society around the world. Ensuring that Canada's research ecosystem serves to advance the public interest requires a deliberate, clear, and shared understanding across all partners of the purpose, use, and ownership of research results. This understanding must be upheld and respected across all stages of the research and in all jurisdictions. Federal research funding for research partnerships must, therefore, be guided not only by scientific merit assessment but also by the appropriate consideration and mitigation of risks to the national security of Canada and the safety of Canadians.

- **Transparency**: Fully transparent and reciprocal sharing of the methods, data, and outcomes of research - while maintaining confidentiality when appropriate - is crucial to research collaboration, integrity, and the free flow of ideas and information. Furthering transparency, the practice of open science may take the form of making scientific inputs, outputs, and processes freely available to all with minimal restrictions. Open science and transparency are practiced in full respect of privacy, security, and ethical considerations, as well as appropriate intellectual property protection, as outlined in Canada's Roadmap for Open Science.

- **Integrity**: As provided for in the Tri-Agency Framework: Responsible Conduct of Research, researchers must strive to follow the best research practices honestly, accountably, openly, and fairly in the search for and in the dissemination of knowledge. This includes respect for the guidance on ethical conduct of research involving humans as well as respecting the rights of those who develop and own intellectual property of any kind throughout the lifecycle of the research project. It also includes the open declaration of all possible conflicts of interest, financial and otherwise, that could impact research outcomes, as well as freedom from any forms of harassment or coercion in the research process that could lead to the mismanagement of conflicts of interest or the fabrication, falsification, plagiarism, or destruction of research records. In addition, researchers must follow the requirements of applicable institutional policies and professional or disciplinary standards and comply with applicable laws and regulations.

- **Collaboration**: Challenging research topics require collaboration with researchers both domestic and international, who bring a diversity of talents, capabilities, and perspectives. In tandem with the principles of academic freedom and institutional autonomy, research collaboration encourages the free flow of ideas and research. Research collaboration must be encouraged and enabled between people, institutions, and organisations who share common research goals and values.

These guidelines will provide clear information on the specific national security considerations for research partnerships. They will enable researchers, research institutions, and government funders to undertake consistent and risk-targeted due diligence to identify and mitigate potential national security risks to research.

The Government of Canada will provide transparent communication and support for this process. The Government of Canada will support the implementation of these guidelines with transparent information, communication, and resources as to the evolving scope and nature of these risks, and how the research community can work to identify and mitigate risks.

What are national security risks in research partnerships?

Research partnerships involve researchers and stakeholders working together on a research project underpinned by a formal partnership agreement (e.g., via a contract or a memorandum of understanding). The process to identify and develop a research partnership based on transparency, shared interests, and mutual benefit can be a lengthy one, involving significant investments of time and resources from all partners.

Foreign governments, militaries, their proxies, and other organizations may seek to exploit research partnerships to access research information (e.g., data), research knowledge, and the resulting intellectual property and technology to facilitate unwanted knowledge transfer. Even when the ultimate intention of the researchers involved may be open knowledge sharing and publication, research partnerships may be exploited in a way that provides privileged and unauthorized access to their research before it is ready to be shared and could compromise sensitive information or research knowledge that is not intended to be publicly available.

These guidelines are intended to help prevent foreign interference, espionage, and unwanted knowledge transfer that could contribute to advancements in the military, security, and intelligence capabilities of states or groups that pose a threat to Canada or that may enable the disruption of the Canadian economy, society, and critical infrastructure.

Unwanted knowledge transfers can also affect the integrity of Canada's research ecosystem by undermining established and shared research practices that include behaving honestly, accountably, openly, and fairly in the search for and in the dissemination of knowledge to the mutual and reciprocal benefit of all partners involved.

What are the elements of possible national security risks in research partnerships?

The elements of national security risks in research partnerships include:

Research area: what are you working on?

- Research that has potential for both military and civilian applications can be considered **dual use** or **sensitive**.

- Sensitive research and its resulting technologies could be used to advance a foreign state's **military, intelligence, or surveillance capabilities** or undermine Canada's national security interests by negatively impacting Canada's capacity to identify and respond to these threats, or by **disrupting the Canadian economy, society, and critical infrastructure**.

- **Influence over and access to data and infrastructure** (both physical and digital), including the data storage, governance, and access provisions of the agreement could be used to support unwanted data access or knowledge transfer outside the scope of the research partnership.

- See Annex A for a list of the sensitive research areas that Canada's national security agencies have identified as having specific potential for dual-use or are targeted by foreign governments, militaries, their proxies, or other actors for the potential to advance national security capabilities and interests.

Partner: who are you working with?

- It is important that you are aware of and assess your partner's goals and objectives for the shared research outcomes. This includes any potential intention or risk to transfer the research knowledge or results to a **foreign government, military, their proxies, or other actors** where doing so may **harm Canada's national security interests.**

- **Partners that are state-owned or subject to state-influence** could facilitate unwanted knowledge transfer in a manner that could harm Canada's national security. Partner organizations that **lack the autonomy and independence** inherent in public research institutions in Canada pose a higher risk of unwanted knowledge transfer to foreign governments, militaries, their proxies, or other actors.

- See Annex B for additional factors that may result in an elevated risk of unwanted knowledge transfer to a foreign government, military, their proxies, or other actors.

How to identify and minimize national security in research partnerships

Identify potential risks:

The process to identify and develop a research partnership based on transparency, shared interests, and mutual benefit can be a lengthy one, involving significant investments of time and resources from both partners.

Therefore, the Government of Canada recommends that researchers undertake due diligence early in the development process, regardless of whether the partners know at the outset if they will eventually be applying for federal research funding.

Researchers should use the *National Security Guidelines for Research Partnerships* to identify potential risks. A complementary risk questionnaire has been developed to assist researchers with this process.

In addition to these guidelines, each research institution will have a range of resources, policies, and processes to help researchers identify and mitigate risks. For any project, especially those with identified national security risks, researchers should use the full range of institutional resources at their disposal to help ensure a successful project; researchers are encouraged to contact their research services or partnerships office for assistance.

Mitigation Measures:

Researchers are encouraged to identify and apply measures that could help minimize any potential or identified national security risks in order to safeguard their research and its outcomes. A strong risk mitigation plan can help decrease the likelihood of potential risks occurring.

Potential measures to help safeguard your research include:

- Building a Strong Research Team,

- Assessing Alignment of Your Partners' Motivations,

- Ensuring Sound Cybersecurity and Data Management Practices; and,

- Agreement on Intended Use of Research Findings, including any commitments to Open Science, Open Data and Open Publication.

All projects are unique and some projects may require additional risk mitigation measures. It is important that all stakeholders in Canada's research ecosystem work collaboratively and in a manner consistent with Canadian laws, to identify, mitigate, and – in cases where the risks to Canadian interests cannot be sufficiently mitigated or outweigh the potential benefits – decline research partnerships that may assist those seeking to undermine Canada's national security.

Implementation:

All researchers are encouraged to protect their work by using the *National Security Guidelines for Research Partnerships* to assess and mitigate risks associated with any potential research partnership.

The *National Security Guidelines for Research Partnerships* will be applied to federal research partnership funding starting with to all applications to the Natural Science and Engineering Research Council's (NSERC) Alliance Grants involving a private sector organization partner. The risk questionnaire and potential mitigation measures will be submitted to and assessed by NSERC, in consultation with national security partners as appropriate. Additional mitigation measures may be required as a prerequisite of funding approval.

Applications for partnerships which are assessed as high risk to national security and/or where risks cannot be appropriately mitigated will not be funded.

Annex A - Sensitive Research Areas

Research Areas Covered by Export Controls

Some fields of research (for example, nuclear, chemical, biological, radiological, or space applications) have a clear link to advancing military or intelligence capabilities and, therefore, have laws and regulations in place that must be followed for the conduct of research and export of any resulting knowledge. For example:

- Research in areas relating to conventional weapons and dual-use goods may be subject to the *Export Control List* (ECL) of the *Export and Import Permits Act* (EIPA) and may require permits prior to transfer of technology to researchers outside of Canada.
- Research in areas related to missile and rocket technology, space technology and chemical and biological weapons and agents may also be subject to the ECL of the EIPA.
- Research in areas involving or applicable to nuclear programs are subject to the EIPA as well as the *Nuclear Non-proliferation Import and Export Control Regulations*.
- Research in areas related to goods or technology identified in the Schedule of the *Defence Production Act* (known as the Controlled Goods List) are sensitive and subject to the *Controlled Goods Program*.
- Research partnerships with institutions and/or researchers located in a country listed on the *Area Control List* of the EIPA must be authorized by an export permit issued by the Minister of Foreign Affairs regardless of the nature of the research.
- Research partnerships with entities sanctioned under the *Special Economic Measures Act* or the *United Nations Act* may require prior authorization from Global Affairs Canada.

Sensitive or Dual-Use Technologies

Some of these laws and regulations do not apply to new and emerging technologies since their potential military, security, and intelligence applications are less clear and well known, and/or because international arms and export control regimes have yet to reach consensus.

These technologies can be **sensitive** or sometimes can be referred to as **dual-use** in that they have military, intelligence, or dual military/civilian applications.

List 1 – Research Areas that may be Considered Sensitive or Dual-Use

- Advanced Materials and Manufacturing
- Advanced Ocean Technologies
- Advanced Sensing and Surveillance
- Advanced Weapons
- Aerospace
- Artificial Intelligence
- Biotechnology
- Energy Generation, Storage and Transmission
- Medical Technology
- Neurotechnology and Human-Machine Integration
- Next Generation Computing and Digital Infrastructure
- Positioning, Navigation and Timing
- Quantum Science
- Robotics and Autonomous Systems
- Space Technology

This list may be updated periodically in accordance with the evolution of technologies, the military and intelligence applications of technology, and national security imperatives.

Additional research areas that can be considered sensitive:

- Research areas related to **critical minerals**, including critical mineral supply chains, on the Government of Canada's *Critical Minerals List*.
- Research areas classified within one of the **critical infrastructure** sectors of the *National Strategy for Critical Infrastructure*. Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety,

security or economic well-being of Canadians and the effective functioning of government.

- Research areas that use **large datasets** that can be analyzed to reveal patterns, trends, and associations, especially related to human behaviour and interactions that may have ethical, commercial, or legal impact on the individual, domestic, or international level. The sensitivity of a large dataset depends on the nature, type, and state of the information it contains, as well as how it may be used in the aggregate.

- Research areas that use **personal data** that could be leveraged by hostile state actors to harm Canada's national and economic security through its exploitation.

List 2 – Examples of Sensitive Personal Data

- Personally identifiable health or genetic (e.g., health conditions or genetic test results);
- Biometric (e.g., fingerprints);
- Financial (e.g., confidential account information, including expenditures and debt);
- Communications (e.g., private communications);
- Geolocation; or,
- Personal data concerning government officials; including members of the military or intelligence community.

Annex B – Partner Risks

It is important for researchers to assess, to the extent they can, the potential for their research partners to contribute to unwanted knowledge transfer for these purposes, either willingly or by compulsion.

The *National Security Guidelines for Research Partnerships* are not aimed at limiting partnerships with any particular country or company. The methods used by individuals and groups who seek to exploit the Canadian research community can be used by any country, or any group, at any time. The Canadian Security Intelligence Service provides public updates including in annual reports, such as the , with examples of activities of foreign governments that are of concern at a specific time; similarly, the Canadian Centre for Cyber Security provides public updates in their National Cyber Threat Assessment. However, threat activities evolve and can originate from anywhere in the world.

Investments by partner organizations that are state-owned or subject to state-influence may be a key indicator of non-commercial interest motivations that could facilitate unwanted knowledge transfer in a manner that could harm Canada's national security. Partner organizations that lack the autonomy and independence similar to public research institutions in Canada pose a greater risk of unwanted knowledge transfer.

Some countries have laws or practices that compel entities and individuals to be subject to direction from their governments to provide Canadian information, research knowledge, technology, and its resulting intellectual property.

Risks can also originate from personnel participating in the project, particularly if individuals have ties to foreign militaries or governments. It is important to identify and assess any potential conflicts of interest and commitment for all individuals involved in a research partnership.